REMARKS

In view of the above amendments and following remarks, reconsideration of the rejections contained in the Office Action of June 4, 2007 is respectfully requested.

The Examiner rejected claims 3, 7, 10, 11, 13-15, 18, 19, 23, 28, 29, 49 and 69-74 as being anticipated by Yang Y R et al.: "Reliable Group Rekeying: A Performance Analysis" (Yang). Further, claims 3-6 and 69 have been rejected as being unpatentable over Wong et al.: "Keystone: A Group Key Management Service" (Wong) in view of Yang. Claims 8 and 9 were further rejected as being unpatentable over Yang in view of Steiner et al.: "Cliques: A New Approach to Group Key Arrangement" (Steiner). Claims 3, 12 and 69 were further rejected as being unpatentable over Paolo, UK 2343025 in view of Yang. Claim 16 was rejected as being unpatentable over Yang in view of Canetti et al.: "Multicast Security: A Taxonomy and Some Efficient Construction" (Canetti). Claims 3, 20-22, 24-27, 34 and 69 were further rejected as being unpatentable Yevgeny, UK 2353682 (Yevgeny) in view of Yang. claims 3, 30-33 and 69 were rejected as being unpatentable over Huang et al.: "Group Leader Election Under-State Routing" (Huang) in view of Yang.

However, while the Applicants do not necessarily acquiesce to the applicability of the above-noted references to the respective claims, each of the independent claims has been proposed to be amended as set forth above. Such amendment clearly distinguishes the present over the cited references in any case.

More specifically, the valid period information as referred to in each of independent claims 49 and 69-74 is now recited as being unique to the member device.

Support for this limitation can for example be found by referring to section 19 beginning at the top of page 66 of the original specification. This section discusses that the registration of the client devices may be restricted by time. For example, "the time between AD server 100 and a client device is synchronized. AD server 100 sets a time period within which use of CSI is permitted as valid period information, transmits the valid period information and CSI to the client device, and add "1" to the registered number.

The client device receives and stores the valid period information and the CSI. When the period shown by the valid period information ends, the client device deletes the CSI.

AD server 100, once the period shown by the valid period information has ended, subtracts "1" from the registered number. If storing the device ID, AD server 100 deletes the ID of the device whose valid period has expired.

Moreover, the usage period information may show a date-time of the start/end of the usage period or only the end date-time. Also, the usage period information may be information that sets restriction on a period from the start of CSI usage, or may set restrictions on a period of operations by a client device using the CSI."

From the above, it is clear that the usage period information that is managed by the AD server can be individually and uniquely set for each client or member device.

New independent claim 75 has also now been proposed. This claim is based on the above description from the original specification, and similarly recites that the valid period information that is issued is unique to the member device.

New dependent claim 76, depending from independent claim 75, recites that the valid period information shows a period in which an off-line device is able to operate as the member device. This is supported in part by the above description, and also by the discussion, for example, beginning at the bottom of page 10 of the original specification: "Also, on-vehicle device 300, although not connected to AD server 100, is able to register as a client device by having CSI stored on IC card 400 and notifying the CSI from IC card 400 to on-vehicle device 300."

With the present invention as now, for example, defined by claim 69, there is recited a judging unit that is operable, upon receiving a request, and if the member device is authenticated as being a legitimate device, to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group, and when judged in the affirmative, to issue a valid period information that is unique to the member device showing a valid period of use of common secret information unique to the group for the member device, and to increase the registered number, and to monitor an elapse of the valid period and reduce the registered number when the valid period ends.

With the structure as recited in claim 69, the group management device of the present application individually sets a valid period for each member device. Accordingly, even if a member

device is not connected on-line with the group management device, the group management device can reduce the registered number of member devices when a valid period that has been set for the member device ends. Further, its possible to reduce the registered number of member devices by performing withdrawal processing in a member device based on a valid period individually set for the member device without performing withdrawal processing upon receiving a voluntary withdrawal request from that member device.

Accordingly, with the device as defined in claim 69, the group management device can always know the precise number of member devices that has been registered in their group that are permitted to use the contents. Furthermore, with the device as defined by claim 69, a flexible system design is possible, because the group management device can set a valid period that is unique to each member device.

Claim 49 is directed to a member device that includes a receiving unit operable to be authenticated by a group management device, and to receive from the group management device, common secret information unique to the group that includes valid period information unique to the member device showing a valid period of use of the common secret information. With the structure as defined in claim 49, the member device can have a set valid period that is unique to that member device. Accordingly, even if the member device is not connected on-line with the group management device, it is possible to delete the common secret information in the member device itself when the valid period that has been set for that member device ends. As such, with the device according to claim 49, contents can be prevented from being used by a member device for an indefinite period.

Each of independent claims 70-75 reflects distinctions similar to those discussed above for claims 69 and 49. All of these claims distinguish over the references that have been cited by the Examiner.

The Examiner initially cites Yang, referring to chapter 4 for tradeoffs of bandwidth overhead and rekey interval for the proposition of issuing valid period information showing a valid period.

However, Yang has the goal of realizing a group rekeying method. When a group key that is common in the group is updated, it is possible to reduce the traffic that is required for updating

the group key by performing batch processing of joined/leave requests received from terminals during a valid period of the group key (rekey interval). Yang thus discloses that terminals are assigned to leaf nodes in a tree structure by using a binary tree structure. When a terminal leaves the group, a newly joined terminal is assigned to an empty leaf node where the previous terminal has left the group. The terminals are assigned to leaf nodes so as not to destroy the tree structure to as great an extent as possible in order to reduce the traffic that is required for updating the group key.

Note that section 2.3 (Periodic Batch Rekeying) and section 2.4 (Bath Rekeying Algorithms) in Yang disclose that periodic batch rekeying is performed efficiently.

The cited chapter 4 (tradeoffs of bandwidth overhead and rekey interval) in Yang discloses what rekey interval is to be set for efficiency in the system. According to this chapter, the system that is disclosed in Yang clearly shows that "a valid period of a common group key distributed to group members is managed."

However, Yang does not disclose or suggest, as recited in claim 69, "a judging unit operable, (i) upon receiving the request, if the member device is authenticated as being a legitimate device, to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group, (ii) when judged in the affirmative, to issue valid period information unique to the member device showing a valid period of use of common secret information unique to the group for the member device, and to increase the registered number, and (iii) to monitor an elapse of the valid period and reduce the registered number when the valid period ends."

For the above reason, Yang does not have the advantage of the present invention in being able to individually set a valid period for each terminal in their group, even if the terminal is not connected on-line with the group management device, and thus does not enable the group management device to reduce the registered number of member devices when a valid period set for that terminal ends. With the present invention, the group management device can always know the precise number of member devices that is registered in the group and are permitted to use the contents.

It is noted that the above distinctions apply similarly to each of the independent claims. Accordingly, it is seen that Yang cannot be considered to anticipate any of the independent claims as now proposed to be amended.

In citing Wong against independent claim 69, the Examiner acknowledged that Wong does not teach the issuance of valid period information showing a valid period of use of the common secret information. However, the Examiner cited Yang for this proposition. Accordingly, the combination of Wong and Yang fails to disclose the present invention as now proposed to be amended, as discussed above.

The Examiner cited Steiner as teaching the common secret information as generated by management device outside the group. However, it does not resolve the above deficiency of the references to Yang and Wong.

In citing Paolo, the Examiner acknowledges that Paolo does not teach the issuance of valid period information showing a valid period of use of the common secret information unique to the group for the member device. However, again, the Examiner cited Yang for this proposition. As such, for the reasons as discussed above, this combination also fails to disclose or render obvious the subject matter of each the independent claims.

The reference to Canetti was cited as teaching a reception unit as receiving a request for withdrawal from the group, etc. However, it fails to cure the above deficiency of Yang, as discussed above.

Yevgeny was also cited by the Examiner to reject independent claim 69. However, the Examiner acknowledged that Yevgeny does not teach the issuance of valid period information showing a valid period of use of common secret information unique to the group for the member device. The reliance upon Yang, as discussed above, does not render this aspect, especially as now claimed, obvious with respect to the present invention.

Claim 69 was also rejected as being unpatentable over Huang, but again reliance was placed upon Yang to teach the issuance of the valid period information showing the valid period of use of the common secret information unique to the group for the member device. Thus, for the reasons

as discussed above, the combination of Huang and Yang does not render obvious the invention as set forth in each of the independent claims.

Accordingly, by the above amendments it is respectfully submitted that all of the prior art references that have been cited by the Examiner fail to disclose or suggest the present invention, and that all of such independent claims are in fact in condition for allowance by such amendment. Accordingly, entry of the amendment and allowance of the application as a whole is respectfully requested.

In view of the above amendments and remarks, it is submitted that the present application is now in condition for allowance, and the Examiner is requested to pass the case to issue. If the Examiner should have any comments or suggestions to help speed the prosecution of this application, the Examiner is requested to contact Applicants' undersigned representative.

Respectfully submitted,

Natsume MATSUZAKI et al.

By: _____

Nils E. Pedersen
Registration No. 33,145
Attorney for Applicants

NEP/krg
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
September 4, 2007